Protecting Data Techniques

TOPIC D – PROTECTING DATA AND INFORMATION

UNIT 1 – INFORMATION TECHNOLOGY SYSTEMS

FARHAN MUKADAM

Techniques for Protecting Data

The best way to protect your data is through implementing simple processes

In the use and administration of IT systems.

- File Permissions
- Access Levels
- Backup & Recovery Procedures
- Passwords
- Physical Access Controls
- Digital Certificates
- Protocols

File Permissions

Files and folders stored on your computer can be set file permissions.

You can set who can access the files and what they can do with them.

Three main types

- **Read Only** – files can be opened and viewed, but not edited.
- **Read/Write** – files can be opened, viewed and edited.
- **Full Control** – files can be opened, viewed, edited, modified & deleted.

Access Level

Similar to file permission but expand beyond just files.

Users are assigned an access level that is associated with their user profile login.

- **Highest Level** - administrator access full control,
- **Lowest Level -** user can only access a limited number of files and software is limited

A key benefit of this to security is in preventing malware from infecting the system.

Backup & Recovery

The biggest impact is the loss of data.

Regular backups of data need to be made

The three main types are:

- **Full Backup** – Complete backup of all your data.
- **Incremental Backup** –Backup only the data that has changed since the previous backup.
- **Differential Backup** – A mixture of the previous two.

Passwords

It is important that we keep our password private

Do not share it with others

Do not write it down.

Guidelines for good password security say that your password should be:

At least 10 characters in length.

Containing uppercase letters, lowercase letters, numbers & symbols.

Do not use the same password repeatedly in different systems.

Physical Access Control

Physical access control includes things like:

- **Access Cards** – Cards that must be scanned to unlock rooms.
- **Keypad Access Control** – A system that requires a passcode to gain entry to a room.
- **Biometric Access Control** – A system that scans biometric data to gain access to a room.
- **Electronic Locks** –lock and unlock doors electronically

Digital Certificates

Used to authenticate a user as the owner of a public key.

A business obtains a digital certificate from a certificate authority.

To get the ‘S’ in HTTPS However, business requires a digital certificate.

Digital Signatures verify the sender’s identity, and their public-key, which is what is used to encrypt data when sending it to the website

Protocols

Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

These protocols provide a secure connection between two computing devices so that data can be transmitted in a secure encrypted format over the internet.

Notes Activity – 20 mins

1. Look through the PowerPoint on Protecting Data Techniques

2. Add **additional** notes for each Data Techniques **2 Bullet Points minimum**

3. Add **1 additional advantage** and **1 disadvantage** for each Data Techniques

4. **Complete activities**

File Permissions

Files and folders stored on your computer can be set file permissions. These can vary from user to user. This basically means that you can set who can access the files and what they can do with them. There are three main types of file permissions you can set.

These are:

- **Read Only** – files can be opened and viewed, but not edited.
- **Read/Write** – files can be opened, viewed and edited.
- **Full Control** – files can be opened, viewed, edited, modified & deleted.

This protects our IT systems from all threats, but particularly hacking and accidental damage. If a user only has read-only access, they cannot edit, modify or delete data, either maliciously or by accident.

File Permissions - Activity

Are there any files in your school that you can only read?

See if you can view the file permission level you have on your own files (this might not be possible in your school).

Access Level

Access levels are closely linked to file permission but expand beyond just files. Users are assigned an access level that is associated with their user profile login. This defines what software, data and services they can access.

At the very highest level, known as administrator access, a user can access all folders with full control, alter the permissions of other users and can install and delete software. At the lowest end, a user can only access a limited number of files and the software they need to do their job.

A key benefit of this to security is in preventing malware from infecting the system. If a user has not got a high enough access level to install software, you do not need to worry about them installing programs that contain malware.

Access Level - Activity

In your school, you will likely find your teachers can access some folders, software & web pages you can’t.

See if you can find out what your different access rights are.

Backup & Recovery

When threats do occur, the biggest impact is the loss of data. If there is a massive data loss, this can often cause a business to fail.

To prevent this, businesses should take regular backups of their data. This involves taking a copy of the data and storing it in a secondary location in case the original data is damaged in some way.

Normally this secondary location is not within the same building. This is known as a “remote” backup and is done in case something happens to the building, such as a fire or flood. If you back up your data to cloud storage, this would be a remote backup.

There are different types of backups procedure too. The three main types are:

- **Full Backup** – This is a complete backup of all your data. This provides excellent protection but is time-consuming and requires huge amounts of data storage capacity to store the backups.
- **Incremental Backup** – This is a backup of only the data that has changed since the previous backup. This is obviously much quicker and requires less storage space than a full backup.
- **Differential Backup** – A mixture of the previous two. A business takes a full backup and then takes backups of data that has changed since that last full backup. So you might do a full backup at the start of each week and then incremental backups each day of the week.

For many businesses, being without their data for a few hours could cost them hundreds of thousands of pounds. These types of businesses will want to have a plan in place to restore the data as quickly as possible. However, smaller businesses may be happier with a slower recovery time.

Backup & Recovery - Activity

Your college will take regular backups and have a recovery procedure.

See if you can find out how regularly backups are taken.

Passwords

Everyone uses passwords to prevent unauthorised users from gaining access to their systems, software and user profiles. It is important that we keep our password private and do not share it with others or write it down as this can easily lead to it being compromised.

Having a good password is particularly important for protection from hackers. However, choosing a simple password is little protection as a hacker can crack simple passwords in seconds. Guidelines for good password security say that your password should be:

- At least 10 characters in length.
- Containing uppercase letters, lowercase letters, numbers & symbols.

It’s also considered best practice to not use the same password repeatedly in different systems. Many users now use a unique password for every user account they own and use a password locker application to remember all of their different passwords.

Passwords - Activity

Visit the web page https://howsecureismypassword.net and see how long your password would take to crack.

Physical Access Control

While passwords control access from a software perspective, we also use physical access controls, particularly in businesses, to protect our IT systems.

Physical access control includes things like:

- **Access Cards** – Cards that must be scanned to unlock rooms. They can be encoded to work on only certain doors and can also be used as identification from security guards (if they contain id information such as a name and photo).
- **Keypad Access Control** – A system that requires a passcode to gain entry to a room. It can be used in place of, or alongside access cards.
- **Biometric Access Control** – A system that scans biometric data to gain access to a room. This might be, for example, fingerprint, iris or facial recognition. Again, this can be used alongside the other above methods to gain access.
- **Electronic Locks** – All the above methods require electronic locks to be used to lock and unlock doors electronically when sent signals from the above access control systems.

This is designed to protect malicious users from gaining access to our IT systems. This helps prevent the theft of equipment, someone loading malware onto a system, and stopping hackers from gaining access to data from within the business' own building.

Physical Access Control - Activity

Why do you think biometrics would be more secure than a keypad?

Why would you not use biometrics?

Digital Certificates

Also known as a public key certificate, this is used to authenticate a user as the owner of a public key. This allows them to make use of the public key infrastructure (PKI) that is used for secure encrypted communications over the internet.

A business obtains a digital certificate from a certificate authority. You've almost certainly used a website where the URL has HTTPS:// as opposed to HTTP:// (there may also be a padlock symbol by the URL too). You probably even know the extra **S** means "secure" and it means the website is encrypting the data being transmitted between you and it.

However, you might not know that to do this, the business requires a digital certificate. You can actually view a websites digital certificate by going through the options settings in your web browser.

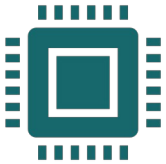
There are several different contents to a digital certificate but the really important bits are the digital signature, which verifies the sender's identity, and their public-key, which is what is used to encrypt data when sending it to the website (such as your login details that you enter in a web form).

Digital Certificates - Activity

Find companies online that provide digital certificates. How much does it cost?

Are there any difficulties in implementing one?

Protocols



As we saw in an earlier lesson, a protocol is a set of rules that defines a method for transmitting data between different devices over a network.

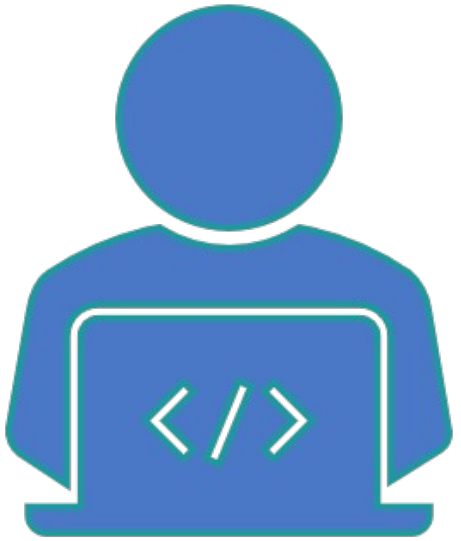
When transmitting data over a network there are specific security protocols. The most commonly used of these are Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

These protocols provide a secure connection between two computing devices so that data can be transmitted in a secure encrypted format over the internet. We looked at this a little bit above, where we said about web pages having HTTPS:// in their URL and this meaning they’re encrypting data. This is SSL/TLS being used.

This, along with the digital certificates we looked at above, ensure that our data, if intercepted by a malicious user, cannot be read and misused.

Protocols - Activity

Why might protocols like SSL/TLS be used in web pages?



Protecting Data Techniques - Summary

File permission means that you can set who can access files and what they can do with them. There are three main file permission types: read-only, read/write and full control.

Access levels control what software, data and services a user can access. The highest level is administrator access.

Backups involve taking a copy of the data and storing it in a secondary location. This is normally in a different building, called a remote backup. There are three main types of backup: full, incremental & differential.

Physical access controls prevent unauthorised users from gaining access to our IT systems. Examples of physical access controls include access cards, keypad access control, biometric access control & electronic locks.

Digital certificates are used to authenticate a user as the owner of a public key so they can use public key encryption. Two key parts of a digital certificate are the signature and the public key.

Protocols are a set of rules that defines a method for transmitting data between different devices over a network. Security protocols that are used include SSL and TLS. These allow us to send data securely over the internet using encryption